On Quasi-Cyclic Codes as a Generalization of Cyclic Codes

Morgan Barbier, Christophe Chabot, Guillaume Quintin

On Quasi-Cyclic Codes as a Generalization of Cyclic Codes

M. Barbier*[1], C. Chabot†[2] and G. Quintin‡[1]

[1]École polytechnique, Laboratoire d'informatique (LIX), 91128 Palaiseau Cedex, France
[2]LJK, 51 rue des mathématiques, Campus de St Martin d'Hères BP 53, 38041 Grenoble Cedex 09, France

May 25, 2012

Abstract

In this article we see quasi-cyclic codes as block cyclic codes. We generalize some properties of cyclic codes to quasi-cyclic codes. We show a one-to-one correspondence between ℓ-quasi-cyclic codes of length $m\ell$ and left ideals of $M_\ell(\mathbb{F}_q)[X]/(X^m - 1)$. Then, we generalize BCH codes and evaluation codes in this context. We study their parameters and establish a key equation. Finally, we present a new $[189, 11, 125]_{\mathbb{F}_4}$ code beating the known minimum distance for fixed length and dimension. Many codes with good parameters beating best known ones have been found from this latter.

1 Introduction

1.1 Context

Many codes with best known minimum distances are quasi-cyclic codes or derived from them [14, 9]. This family of codes is therefore very interesting. Quasi-cyclic codes were studied and applied in the context of McEliece's cryptosystems [16, 2] and Niederreiter's [17, 12]. They permit to reduce the size of keys in opposition to Goppa codes. However, since the decoding of random quasi-cyclic codes is difficult, only quasi-cyclic alternant codes were proposed for the latter cryptosystems. The high structure of alternant codes is actually a weakness and two cryptanalyses were proposed in [7, 18]. For these reasons,

*morgan.barbier@lix.polytechnique.fr
†christophechabotcc@gmail.com
‡quintin@lix.polytechnique.fr

studying the decoding methods and the general properties of quasi-cyclic codes are interesting topics.

The structure of quasi-cyclic codes has been studied in different ways. In [10], quasi-cyclic codes are regarded as concatenation of cyclic codes, while in [13], the authors regard them as linear codes over an auxiliary ring. In [5], the approach is more analogous to the cyclic case. The authors consider the factorization of $X^m - 1 \in M_\ell(F_q)[X]$ with reversible polynomials in order to construct ℓ-quasi-cyclic codes canceled by those polynomials and called $\Omega(P)$-codes. This leads to the construction of self-dual codes and codes beating known bounds. But the factorization of univariate polynomials over a matrix ring remains difficult. In [6] the author gives an improved method for particular cases of the latter factorization problem.

In this article, we prove, analogously to the cyclic case, a one-to-one correspondence between ℓ-quasi-cyclic codes of length $m\ell$ and left ideals of $M_\ell(F_q)[X]/(X^m - 1)$. We study the properties of quasi-cyclic codes and propose to extend the definition of BCH and evaluation codes to the context of quasi-cyclic codes. Namely, we define *quasi-BCH* and *quasi-evaluation* codes. The natural notion of *folded* and *unfolded* codes is presented for simplicity and decoding purposes. Finally, we exhibit a quasi-cyclic code whose parameters are better than the previous known and 48 other codes derived from the first one.

Subsection 1.2 is devoted to some recalls about $\Omega(P)$-codes and definitions. Then in Section 2 we prove interesting properties about quasi-cyclic codes and, in particular, the correspondence between left ideals and quasi-cyclic codes. Section 3 deals with the definition, parameters and a decoding algorithm of quasi-BCH codes. Finally, Section 5 introduces quasi-evaluation codes and gives lower bounds on their parameters.

1.2 First definitions

In this section, we fix a positive integer n and let $\mathcal{C}$ be a code of length n over the finite field $\mathbb{F}_q$, *i.e.* a vector subspace of $\mathbb{F}_q^n$.

Definition 1 (Quasi-cyclic codes)**.** From now and until the end of this article we define $T : \mathbb{F}_q^n \to \mathbb{F}_q^n$ to be the left cyclic shift defined by:

$$T(c_1, c_2, \ldots, c_n) = (c_2, c_3, \ldots, c_1).$$

Suppose that ℓ divides n. Then we call an *ℓ-quasi-cyclic code over $\mathbb{F}_q$ of length n* a code of length n over $\mathbb{F}_q$ stable by T^ℓ. If the context is clear we will simply say *ℓ-quasi-cyclic code*.

Let ℓ be an integer, and $\alpha \in \mathbb{F}_{q^\ell}$ be such that $(1, \alpha, \ldots, \alpha^{\ell-1})$ is an $\mathbb{F}_q$-base of the vector space $\mathbb{F}_{q^\ell}$. We define the *folding* to be the $\mathbb{F}_q$-linear map

$$\begin{array}{rcl} \phi : \mathbb{F}_q^\ell & \to & \mathbb{F}_{q^\ell} = \mathbb{F}_q[\alpha] \\ (a_1, \ldots, a_\ell) & \mapsto & a_1 + a_2\alpha + \cdots + a_\ell \alpha^{\ell-1}. \end{array}$$

The unfolding is the inverse $\mathbb{F}_q$-linear map

$$\begin{array}{rcl} \phi^{-1}: \mathbb{F}_{q^\ell} & \to & \mathbb{F}_q^\ell \\ a = a_1 + a_2\alpha + \cdots + a_\ell \alpha^{\ell-1} & \mapsto & (a_1, a_2, \ldots, a_\ell). \end{array}$$

Let m be a positive integer, $f : E \to F$ be any map of sets. We denote by $f^{\times m}$ the map of sets $f^{\times m} : E^m \to F^m$ such that $f^{\times m}(x_1, \ldots, x_m) = (f(x_1), \ldots, f(x_m))$.

Definition 2 (Folded and unfolded codes)**.** Suppose that $n = m\ell$. We define the *folded code* of $\mathcal{C}$ to be $\phi^{\times m}(\mathcal{C})$. Let $\mathcal{C}'$ be a code in $\mathbb{F}_{q^\ell}^m$. We define the *unfolded code* of $\mathcal{C}'$ to be $(\phi^{-1})^{\times m}(\mathcal{C}')$.

Remark 3. Observe that a code $\mathcal{C}$ is ℓ-quasi cyclic if and only if its folded $\mathcal{C}' = \phi^{\times m}(\mathcal{C})$ is cyclic. But $\mathcal{C}'$ is not necessarily $\mathbb{F}_{q^\ell}$-linear.

2 Properties of quasi-cyclic codes

In the present section we generalize the results of [15, Theorem 1, page 190] to quasi-cyclic codes. We fix a positive integer n and suppose that $n = m\ell$ for two positive integers m and ℓ.

2.1 The one-to-one correspondence

It is well-known [15, Theorem 1, page 190] that there is a one-to-one correspondence between cyclic codes of length n over $\mathbb{F}_q$ and monic factors of $X^n - 1 \in \mathbb{F}_q[X]$ *i.e.* ideals of $\mathbb{F}_q[X]/(X^n - 1)$. In [5, 6] the authors start to exhibit such a correspondence for quasi-cyclic codes. They show that there is a correspondence between a subfamily of ℓ-quasi-cyclic codes of length $m\ell$ over $\mathbb{F}_q$ and reversible factors of $X^n - 1 \in M_\ell(\mathbb{F}_q)[X]$.

The one-to-one correspondence between ℓ-quasi cyclic codes and left ideals of $M_\ell(\mathbb{F}_q)[X]/(X^m - 1)$ is a consequence of the two following lemmas.

Lemma 4. *Let R be a commutative principal ring and M be a free left module of finite rank s over R. Then every submodule N of M can be generated by at most s elements.*

Proof. It is an easy adaptation of the proof of [11, Theorem 7.1, page 146]. □

Lemma 5. *Let s be a positive integer and R be a commutative principal ring. Then there is a one-to-one correspondence between the submodules of R^s and the left ideals of $M_s(R)$.*

Proof. Note that this is a particular case of the Morita equivalence for modules. See for example [4, n°4, page 99]. This particular case can be proved directly. To a submodule $N \subseteq R^s$, we can build a left ideal of $M_s(R)$ whose elements have rows in N. Conversely, to a left ideal $I \subseteq M_s(R)$ we associate the submodule of R^s generated by all the rows of all the elements of I. It is straightforward to check that these maps are inverse to each other. □

Note that $M_\ell(\mathbb{F}_q)[X]/(X^m-1)$ and $M_\ell(\mathbb{F}_q[X]/(X^m-1))$ are isomorphic as rings and that $R = \mathbb{F}_q[X]/(X^m-1)$ is a commutative principal ring. By Lemma 4 any submodule of R^ℓ can be generated by at most ℓ elements. Therefore by Lemma 5 any left ideal of $M_\ell(R) = M_\ell(\mathbb{F}_q)[X]/(X^m-1)$ is principal.

Theorem 6. *There is a one-to-one correspondence between ℓ-quasi-cyclic codes over $\mathbb{F}_q$ of length $m\ell$ and left ideals of $M_\ell(\mathbb{F}_q)[X]/(X^m-1)$.*

Proof. Let $g = (g_{11}, \ldots, g_{1\ell}, g_{21}, \ldots, g_{2\ell}, \ldots, g_{m1}, \ldots, g_{m\ell}) \in \mathbb{F}_q^{m\ell}$. We associate to g the element $\varphi(g) \in (\mathbb{F}_q[X]/(X^m-1))^\ell$ defined by

$$\begin{aligned}\varphi(g) = \big(g_{11} + g_{21}X + \cdots + g_{m1}X^{m-1};&\\ g_{12} + g_{22}X + \cdots + g_{m2}X^{m-1}; \ldots;&\\ g_{1\ell} + g_{2\ell}X + \cdots + g_{m\ell}X^{m-1}\big)&.\end{aligned}$$

Then φ induces a one-to-one correspondence between ℓ-quasi-cyclic codes of length $m\ell$ over $\mathbb{F}_q$ and submodules of $(\mathbb{F}_q[X]/(X^m-1))^\ell$. The theorem follows by Lemma 5. ☐

Let $\mathrm{pr}_{i,j}$ be the projection of the $i, i+1, \ldots, j$ coordinates:

$$\begin{array}{rcl}\mathrm{pr}_{i,j} : \mathbb{F}_q^n & \longrightarrow & \mathbb{F}_q^{j-i+1}\\ (x_1, \ldots, x_n) & \longmapsto & (x_i, x_{i+1}, \ldots, x_{j-1}, x_j).\end{array}$$

We have the following obvious lemma:

Lemma 7. *Let $\mathcal{C}$ be an ℓ-quasi-cyclic code over $\mathbb{F}_q$ of dimension k and length $m\ell$. Then there exists an integer r such that $1 \le r \le k$ and for any generator matrix G of $\mathcal{C}$ and $0 \le i \le m-1$, the rank of the $i\ell+1, i\ell+2, \ldots, (i+1)\ell$ columns of G is r.*

Definition 8 (Block rank)**.** Taking the notation of Lemma 7, we call the integer r the *block rank* of $\mathcal{C}$. Note that r depends only on $\mathcal{C}$ and not on any particular generator matrix of $\mathcal{C}$.

2.2 The generator polynomial of an ℓ-quasi-cyclic code

In this subsection we fix an ℓ-quasi-cyclic code $\mathcal{C}$ over $\mathbb{F}_q$. If $\ell = 1$, then $\mathcal{C}$ is a cyclic code of length n and a generator matrix of $\mathcal{C}$ can be given [15, Theorem 1, (e), page 191] by

$$\begin{pmatrix} g(X) & & & \\ & Xg(X) & & \\ & & \cdots & \\ & & & X^{n-\deg g}g(X) \end{pmatrix}, \tag{1}$$

where $g(X) \in \mathbb{F}_q[X]$ is the generator polynomial of $\mathcal{C}$. The block rank of $\mathcal{C}$ is 1 and we see that we can write a generator matrix of $\mathcal{C}$ with only 1 vector and its shifts (by $T^\ell = T$). The natural generalization of this result for quasi-cyclic codes is done using the block rank.

Let r be the block rank of $\mathcal{C}$, the following algorithm computes a basis of $\mathcal{C}$ from r vectors of $\mathcal{C}$ and their shifts. We call the *first index* of a nonzero vector $x = (x_1, \dots, x_{m\ell})$ the least integer $0 \leq i \leq m-1$ such that $(x_{i\ell+1}, \dots, x_{(i+1)\ell}) \neq 0$ and denote it by $\mathcal{F}(x) = \mathcal{F}(x_1, \dots, x_{m\ell})$. Let

$$\begin{array}{rcc} p : \mathbb{F}_q^{m\ell} & \longrightarrow & \mathbb{F}_q^{\ell} \\ x = (x_1, \dots, x_{m\ell}) & \longmapsto & (x_{i\ell+1}, \dots, x_{(i+1)\ell}), \end{array}$$

where $i = \mathcal{F}(x_1, \dots, x_n)$ if $x \neq 0$ and $p(0) = 0$.

Algorithm 2.1 Basis computation with the block rank

Input: A generator matrix G of $\mathcal{C}$.
Output: A generator matrix formed by r rows from G and some of their shifts.
$G' \leftarrow$ a row echelon form of G.
Denote by $g_1, \dots, g_k$ the rows of G'.
$M \leftarrow \max\{\mathcal{F}(g_i) : i \in \{0, \dots, m-1\}\}$.
$B'_M \leftarrow \emptyset$.
$G_{M+1} \leftarrow \emptyset$.
for $j = M \to 0$ **do**
    $B_j \leftarrow \{g_i : i \in \{1, \dots, k\}$ and $\mathcal{F}(g_i) = j\}$.
    for each element x of B_j **do**
        if $p(B'_j) \cup \{p(x)\}$ are independent **then**
            $B'_j \leftarrow B'_j \cup \{x\}$.
        end if
    end for
    $G_j \leftarrow G_{j+1} \cup B'_j$.
    $B'_{j-1} \leftarrow T^\ell(B'_j)$.
end for
return G_0.

Note that Algorithm 2.2 applied to a cyclic code, *i.e.* $\ell = 1$, returns exactly the matrix (1) and we can deduce the generator polynomial of $\mathcal{C}$ at the cost of the computation of a row echelon form of any generator matrix of $\mathcal{C}$.

Proposition 9. *Algorithm 2.2 works correctly as expected and returns a generator matrix G of $\mathcal{C}$ made of r linearly independent vectors of $\mathcal{C}$ and some of their shifts.*

Proof. We will prove by descending induction on j that:

1. $B'_j \supseteq T^\ell(B'_{j+1}) \supseteq \cdots \supseteq T^{(M-j)\ell}(B'_M)$.
2. $\#B'_j \leq r$.
3. The vectors of B'_j are linearly independent.

4. The vectors of G_j are linearly independent.

5. $\langle G_j \rangle = \langle g_i : i \in \{1, \ldots, k\}$ and $\mathcal{F}(g_i) \geq j \rangle$.

Let $j = M$. By step 3, we have $B_M \neq \emptyset$. Item 1 is trivially satisfied. By Lemma 7, $\# B_M \leq r$ and item 2 is satisfied. As $G_{M+1} = B'_M = \emptyset$ then $G_M = B'_M = B_M = \{g_i : i \in \{1, \ldots, k\}$ and $\mathcal{F}(g_i) \geq M\}$ and items 3 to 5 are satisfied.

Suppose that $j < M$ and that items 1 to 5 are satisfied for $i = j+1, \ldots, M$. First note that $B_j \neq \emptyset$. If we had $B_j = \emptyset$ then, as G' is in row echelon form, $g_1, \ldots, g_k, T^{(M-j)\ell}(g_k)$ would be linearly independent which is a contradiction.

Items 1 and 3 are satisfied by steps 7, 9 and 10 of the algorithm. By Lemma 7 and step 9, item 2 is satisfied. For all $x \in G_{j+1}$, we have $\mathcal{F}(x) \geq j+1$, thus, by item 3, the elements of G_j are linearly independent and item 4 is satisfied. Let g be a vector of G' such that $\mathcal{F}(g) = j$, then the construction of B'_j implies that we have

$$\mathcal{F}\left(g - \sum_{u \in B'_j} \mu_u u\right) \geq j+1$$

where $\mu_u \in \mathbb{F}_q$ for $u \in B'_j$. Then by item 5 of the inductive hypothesis, we have

$$\left(g - \sum \mu_u u\right) \in G_{j+1}.$$

Thus we have $\langle G_j \rangle = \langle g_i : i \in \{1, \ldots, k\}$ and $\mathcal{F}(g_i) \geq j \rangle$ and item 5 is satisfied.

As a consequence of the previous induction, G_0 is constituted of linearly independent vectors and generates $\langle g_i : i \in \{1, \ldots, k\}$ and $\mathcal{F}(g_i) \geq 0 \rangle = \mathcal{C}$ by item 5. By Lemma 7 we must have exactly r vectors $g \in G_0$ such that $\mathcal{F}(g) = 0$. Thus by items 1 and 2 we have

$$r = \# B'_0 = \sum_{\lambda=0}^{M} \# \left(B'_\lambda \setminus T^\ell(B'_{\lambda+1})\right)$$

which shows that G_0 is constituted of r linearly independent vectors of $\mathcal{C}$ and some of their shifts. $\square$

Corollary 10. *There exist $g_1, \ldots, g_r$ linearly independent vectors of $\mathcal{C}$ such that $g_1, \ldots, g_r, T^\ell(g_1), \ldots, T^\ell(g_r), \ldots, T^{(m-1)\ell}(g_1), \ldots, T^{(m-1)\ell}(g_r)$ span $\mathcal{C}$. If we denote by $g_{i,j}$ the j'th coordinate of g_i and let*

$$G_i = \begin{pmatrix} g_{1,i\ell+1} & \cdots & g_{1,(i+1)\ell} \\ \vdots & & \vdots \\ g_{r,i\ell+1} & \cdots & g_{r,(i+1)\ell} \\ & 0 & \end{pmatrix} \in M_\ell(\mathbb{F}_q)$$

and

$$g(X) = \frac{1}{X^\nu} \sum_{i=0}^{m-1} G_i X^i \in M_\ell(\mathbb{F}_q)[X],$$

where ν is the least integer such that $G_i \neq 0$, then $\mathcal{C}$ corresponds to the left ideal $\langle g(X)\rangle$ by Theorem 6.

Corollary 11. *Taking the notation of the proof of Theorem 6, the submodule $\varphi(\mathcal{C}) \subseteq (\mathbb{F}_q[X]/(X^m-1))^\ell$ is generated by r elements as an $\mathbb{F}_q[X]/(X^m-1)$-module but cannot be generated by less that r elements. If $\mathcal{C}$ is a cyclic code then we have $r=1$ and we find the classical result about cyclic codes.*

Definition 12 (Generator polynomial)**.** The polynomial $g(X) \in M_\ell(\mathbb{F}_q)[X]$ from Corollary 10 is called a *generator polynomial* of $\mathcal{C}$.

Example 13. Let $I = \langle P(X), Q(X)\rangle \subset M_3(\mathbb{F}_4)[X]/(X^5-1)$ be a left ideal. The row echelon form generator matrix of the 3-quasi cyclic code $\mathcal{C}_I$ associated to the left ideal I is

$$G = \left(\begin{array}{ccc|ccc|ccc|ccc|ccc} 1 & 0 & \omega^2 & 0 & 0 & 0 & 0 & \omega^2 & \omega & \omega & 0 & 1 & 0 & 0 & 0 \\ 0 & 1 & \omega^2 & 0 & 0 & 0 & 0 & 0 & 0 & \omega & \omega & 0 & 1 & 0 & \omega^2 \\ \hline 0 & 0 & 0 & 1 & 0 & \omega^2 & 0 & 0 & 0 & 0 & \omega^2 & \omega & \omega & 0 & 1 \\ 0 & 0 & 0 & 0 & 1 & \omega^2 & 0 & \omega^2 & \omega & \omega & 0 & 1 & \omega & \omega & 0 \\ \hline 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 0 & \omega^2 & 0 & \omega & 0 & \omega^2 & \omega \end{array}\right).$$

Algorithm 2.2 gives that $(g_4, g_5, T^3(g_4), T^3(g_5), T^{2\times 3}(g_5))$ is a basis of $\mathcal{C}_I$. Moreover

$$g(X) = \begin{pmatrix} 0 & 1 & \omega^2 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix} + \begin{pmatrix} 0 & \omega^2 & \omega \\ 1 & 1 & 0 \\ 0 & 0 & 0 \end{pmatrix} X + \begin{pmatrix} \omega & 0 & 1 \\ \omega & 0 & \omega \\ 0 & 0 & 0 \end{pmatrix} X^2 + \begin{pmatrix} \omega & \omega & 0 \\ 0 & \omega^2 & \omega \\ 0 & 0 & 0 \end{pmatrix} X^3$$

is a generator polynomial of $\mathcal{C}_I$ and $I = \langle P(X), Q(X)\rangle = \langle g(X)\rangle$.

2.3 A property of generator polynomials

The following proposition generalizes [15, Theorem 1, (c), page 190] and [15, Theorem 4, page 196].

Proposition 14. *Let $\mathcal{C}$ be an ℓ-quasi-cyclic code of length $m\ell$ over $\mathbb{F}_q$. Let $P(X)$ be a generator polynomial of $\mathcal{C}$ and $Q(X)$ a generator polynomial of its dual. Then*

$$P(X)\left({}^tQ^\star(X)\right) = 0 \pmod{X^m - 1}$$

where $Q^\star$ denotes the reciprocal polynomial of Q and ${}^tQ$ the polynomial whose coefficients are the transposed matrices of the coefficients of Q.

Proof. Since $P(X) = \sum_{i=0}^{m-1} P_i X^i$ is a generator polynomial of $\mathcal{C}$, the rows of the matrix

$$\begin{pmatrix} P_0 & P_1 & \dots & P_{m-1} \end{pmatrix}$$

and their shifts span $\mathcal{C}$. Similarly $Q(X) = \sum_{i=0}^{m-1} Q_i X^i$ and the rows of

$$\begin{pmatrix} Q_0 & Q_1 & \dots & Q_{m-1} \end{pmatrix}$$

and their shifts span $\mathcal{C}^{\perp}$. By definition of a dual code, we have

$$\begin{pmatrix} P_0 & P_1 & \cdots & P_{m-1} \end{pmatrix} \begin{pmatrix} {}^tQ_0 \\ {}^tQ_1 \\ \vdots \\ {}^tQ_{m-1} \end{pmatrix} = \sum_{i=0}^{m-1} P_i \left({}^tQ_i\right) = 0.$$

As $\mathcal{C}$ and $\mathcal{C}^{\perp}$ are ℓ-quasi cyclic codes we also have

$$\sum_{i=0}^{m-1} P_i \left({}^tQ_{i+j \mod m}\right) = 0$$

for all $j \in \mathbb{Z}$. Therefore

$$P(X)\left({}^tQ^{\star}(X)\right) = \sum_{j=0}^{m-1}\sum_{i=0}^{m-1} P_i \left({}^tQ_{i-j \mod m}\right) X^j = 0 \mod (X^m - 1).$$

Hence the proposition. □

3 Quasi-BCH

In Section 2 we saw that quasi-cyclic codes can be regarded as a generalization of cyclic codes. Therefore, it is interesting to focus on the generalization of BCH codes. We start with the definition and then study their parameters. Finally we present a decoding scheme for quasi-BCH codes raising interesting questions. We fix four positive integers $n = m\ell$ and s.

3.1 Definition

Definition 15 (Primitive root of unity)**.** Let q be a prime power. A matrix $A \in M_\ell(\mathbb{F}_{q^s})$ is called a *primitive m-th root of unity* if

- $A^m = I_\ell$,
- $A^i \neq I_\ell$ if $i < m$,
- $\det(A^i - A^j) \neq 0$, whenever $i \neq j$.

Proposition 16. *Let q be a prime power and suppose that $q^{s\ell} - 1 = m$. Then there exists a primitive m-th root of unity in $M_\ell(\mathbb{F}_{q^s})$.*

Proof. Let $\alpha \in \mathbb{F}_{q^{s\ell}}$ be a primitive m-th root of unity and $A \in M_\ell(\mathbb{F}_{q^s})$ be the companion matrix of the irreducible polynomial $f(X) \in \mathbb{F}_{q^s}[X]$ of α over $\mathbb{F}_{q^s}$. There exists $P \in \mathrm{GL}_\ell(\mathbb{F}_{q^{s\ell}})$ and an upper triangular matrix $U \in M_\ell(\mathbb{F}_{q^{s\ell}})$ whose diagonal coefficients are the eigenvalues of A such that $A = P^{-1}UP$. The eigenvalues of A are exactly the roots of f and then are primitive m-th roots of unity. Therefore A satisfies the three conditions of Definition 15. □

Definition 17 (Block minimum distance)**.** Let $\mathcal{C}$ be a linear code over $\mathbb{F}_q$ of length $m\ell$. We define the *ℓ-block minimum distance* of $\mathcal{C}$ to be the minimum distance of the folded code of $\mathcal{C}$.

Definition 18 (Left quasi-BCH codes)**.** Let A be a primitive m-th root of unity in $M_\ell(\mathbb{F}_{q^s})$ and $\delta \leq m$. We define the ℓ-quasi-BCH code of length $m\ell$, with respect to A, with designed minimum distance δ, over $\mathbb{F}_q$ by

$$\text{Q-BCH}_q(m, \ell, \delta, A) := \left\{ (c_1, \ldots, c_m) \in (\mathbb{F}_q^\ell)^m : \sum_{j=0}^{m-1} A^{ij} c_j = 0 \text{ for } i = 1, \ldots, \delta - 1 \right\}.$$

We call the linear map

$$\begin{array}{rcl} \mathcal{S}_A : (\mathbb{F}_q^\ell)^m & \to & (\mathbb{F}_{q^s}^\ell)^m \\ x = (x_1, \ldots, x_m) & \mapsto & \sum_{j=0}^{m-1} A^j x_j \end{array}$$

the *syndrome* map with respect to $\text{Q-BCH}(m, \ell, \delta, A)$.

Proposition 19. *Using the notation of Definition 18,* $\text{Q-BCH}_q(m, \ell, \delta, A)$ *has dimension at least* $(m - e(\delta - 1))\ell$ *and ℓ-block minimum distance at least δ. In other words* $\text{Q-BCH}_q(m, \ell, \delta, A)$ *is an* $[m\ell, \geq (m - s(\delta - 1))\ell, \geq \delta]_{\mathbb{F}_q}$*-code.*

Proof. According to Definition 18 we have that

$$H = \begin{pmatrix} I_\ell & A & \cdots & A^{m-1} \\ I_\ell & A^2 & \cdots & A^{2(m-1)} \\ \vdots & \vdots & & \vdots \\ I_\ell & A^{\delta-1} & \cdots & A^{(\delta-1)(m-1)} \end{pmatrix} \in M_{(\delta-1)\ell, m\ell}(\mathbb{F}_{q^s})$$

is a parity check matrix of $\text{Q-BCH}_q(m, \ell, \delta, A)$. Let

$$V = \begin{pmatrix} I_\ell & A & \cdots & A^{\delta-1} \\ I_\ell & A^2 & \cdots & A^{2(m-1)} \\ \vdots & \vdots & & \vdots \\ I_\ell & A^{\delta-1} & \cdots & A^{(\delta-1)^2} \end{pmatrix}.$$

Using the Vandermonde matrix trick we find that the determinant D of V over $M_\ell(\mathbb{F}_{q^s})[A]$ is $\prod_{i<j}(A^i - A^j)$. By the definition of A we have $\det_{\mathbb{F}_{q^s}} D \neq 0$, thus V is invertible over $M_\ell(\mathbb{F}_{q^s})[A]$ and then, invertible over $\mathbb{F}_{q^s}$. Therefore H has full rank over $\mathbb{F}_{q^s}$.

Let $i : \mathbb{F}_q^{m\ell} \to \mathbb{F}_{q^s}^{m\ell}$ be the canonical injection and denote by $h : \mathbb{F}_{q^s}^{m\ell} \to \mathbb{F}_{q^s}^{(\delta-1)\ell}$ the $\mathbb{F}_q$-linear map given by H. Then we have $\dim_{\mathbb{F}_q}(\operatorname{Im} h) = e(\delta - 1)\ell$. Thus $\dim_{\mathbb{F}_{q^s}}(\operatorname{Im} h \circ i) \leq (\delta - 1)\ell$ and $\dim_{\mathbb{F}_q}(\operatorname{Im} h \circ i) \leq e(\delta - 1)\ell$. Therefore $\dim_{\mathbb{F}_q}(\ker h \circ i) \geq m\ell - e(\delta - 1)\ell$. Suppose that there exists a codeword

$c = (c_1, \dots, c_m) \in \mathcal{C} \setminus \{0\}$ with ℓ-block weight $b \le \delta - 1$. Note $i_1, \dots, i_b$ the indexes such that $c_{i_j} \neq 0$ for $i = 1, \dots, b$. This implies that the matrix

$$\begin{pmatrix} A^{i_1} & A^{i_2} & \dots & A^{i_b} \\ A^{2i_1} & A^{2i_2} & \dots & A^{2i_b} \\ \vdots & \vdots & & \vdots \\ A^{(\delta-1)i_1} & A^{(\delta-1)i_2} & \dots & A^{(\delta-1)i_b} \end{pmatrix}$$

has not full rank which is absurd. □

Example 20. Consider the 3-quasi-BCH codes defined by primitive roots in $M_3(\mathbb{F}_{2^2})$ of length 63 over $\mathbb{F}_2$ with designed minimum distance 6 defined by a 21-th root of unity in $\mathbb{F}_{2^2}$. In other words, $q = 2, m = 21, \ell = 3, s = 2$ and $\delta = 6$. There are 22 non-equivalent codes splitting as follows:

Number of codes	Parameters
2	$[63, 33, 6]_{\mathbb{F}_2}$
18	$[63, 33, 7]_{\mathbb{F}_2}$
2	$[63, 36, 6]_{\mathbb{F}_2}$

Notice that their dimension is always at least $(m - e(\delta - 1))\ell = 33$ and their minimum distance is at least $\delta = 6$. All the computations have been performed with the MAGMA computer algebra system [3].

Example 21. Let $q = 5, m = 7, \ell = 3, s = 2$ and $\delta = 3$. Let $\omega \in \mathbb{F}_{5^2}$ be a primitive $(5^2 - 1)$-th root of unity and

$$A = \begin{pmatrix} \omega^9 & \omega^4 & \omega^{22} \\ \omega^{11} & \omega^{11} & \omega^{15} \\ \omega^2 & \omega^{19} & 1 \end{pmatrix} \in M_3(\mathbb{F}_{5^2}).$$

Then the left 3-quasi-BCH code of length 21 with respect to A with designed minimum distance 3 over $\mathbb{F}_5$ has parameters $[21, 9, 7]_{\mathbb{F}_5}$. Its generator polynomial is given by

$$g(X) = \begin{pmatrix} 1 & 4 & 3 \\ 3 & 3 & 4 \\ 1 & 1 & 4 \end{pmatrix} X^4 + \begin{pmatrix} 4 & 0 & 0 \\ 4 & 0 & 0 \\ 4 & 0 & 4 \end{pmatrix} X^3 + \begin{pmatrix} 3 & 0 & 4 \\ 0 & 3 & 4 \\ 0 & 0 & 0 \end{pmatrix} X^2 + \begin{pmatrix} 2 & 3 & 2 \\ 4 & 4 & 4 \\ 3 & 1 & 1 \end{pmatrix} X + \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \in M_3(\mathbb{F}_5)[X].$$

4 Decoding scheme for quasi-BCH codes

For this section we fix five positive integers $n = m\ell$, r and δ, a primitive m-th root of unity $A \in M_\ell(\mathbb{F}_{q^s})$ and $\mathcal{C} = \text{Q-BCH}(m, \ell, \delta, A)$. If the folded of $\mathcal{C}$ is a BCH code $\mathcal{C}'$ over $\mathbb{F}_{q^\ell}$ (which is not the case in general) then we can apply the standard, unique and list, decoding algorithms. See for example [15, Paragraph 6, page 270] and [1]. If $\mathcal{C}'$ is not a code for which a decoding algorithm is known, we propose in what follows a decoding scheme for $\mathcal{C}$ based on the key equation that we establish for quasi-BCH codes. Following the same techniques as for BCH codes, we first compute the locator and evaluator polynomials by solving the key equation and then compute the error vector and recover the original message.

Notation 22. Let κ be any field and $x = (x_1, \ldots, x_n) \in \kappa^n$. We denote by $w(x)$ the Hamming weight of x *i.e.* the cardinal of $W = \{i : i \in \{1, \ldots, n\} \text{ s.t. } x_i \neq 0\}$. We denote by $\mathrm{Supp}(x)$ the support of x *i.e.* the set W.

4.1 The key equation

As in the scalar case, we exhibit a key equation for quasi-BCH codes. In this subsection, all vectors are considered to be single-column matrices. Consider $\mathbb{F}_q^\ell$ as a product ring of ℓ copies of $\mathbb{F}_q$. We define a map

$$\begin{array}{rcl} \Psi : M_\ell(\mathbb{F}_{q^s})[[X]] \times \mathbb{F}_q^\ell[[X]] & \to & \mathbb{F}_{q^s}^\ell[[X]] \\ (f, g) & \mapsto & \sum_{i,j} f_j g_i X^{i+j} \end{array}$$

where the $f_i g_j$ are matrix-vector products. In the sequel we will denote $\Psi(f, g)$ simply by $f \diamond g$. Note that we have $(fh) \diamond g = f \diamond (h \diamond g)$ for any $h \in M_\ell(\mathbb{F}_{q^s})$.

Let c be a codeword of $\mathcal{C}$ sent over a channel, $y \in (\mathbb{F}_q^\ell)^m$ be the received word and let e be the error vector *i.e.* $e = y - c$ such that $\mathrm{w}(e) = w \leq \lfloor (\delta - 1)/2 \rfloor$. Let $W = \mathrm{Supp}(e) = \{i_1, \ldots, i_w\}$.

Definition 23 (Locator and evaluator polynomials)**.** We define the *locator polynomial* by

$$\Lambda(X) := \prod_{i \in W} (1 - A^i X) \in M_\ell(\mathbb{F}_{q^s})$$

and the *evaluator polynomial* by

$$L(X) := \sum_{i \in W} \left(\prod_{j \neq i}^{w} A^i (1 - A^j) X \right) \diamond y_i \in \mathbb{F}_{q^s}^\ell[X].$$

Lemma 24. *Let $B \in M_\ell(\mathbb{F}_q)$ be a nonzero matrix, then $1 - BX$ has a left- and right- inverse in $M_\ell(\mathbb{F}_q)[[X]]$, both equal to*

$$\sum_{j=0}^{+\infty} B^j X^j.$$

We see that the locator polynomial $\Lambda(X)$ is invertible in the power series ring $M_\ell(\mathbb{F}_{q^s})[[X]]$ and we have

$$\begin{aligned}\left(\Lambda(X)^{-1}\right)\diamond L(X) &= \sum_{i\in W}\left(A^i(1-A^iX)^{-1}\right)\diamond y_i\\ &= \sum_{i\in W}\left(\sum_{j=0}^{+\infty}A^{i(j+1)}X^j\right)\diamond y_i\\ &= \sum_{j=0}^{+\infty}\sum_{i\in W}A^{i(j+1)}y_iX^j.\end{aligned}$$

Using the fact that $y = c + e$ and that, by definition, $\mathcal{S}_{A^i}(y) = \mathcal{S}_{A^i}(e)$ for any $i = 0, \dots, \delta - 1$ we have

$$\left(\Lambda(X)^{-1}\right)\diamond L(X) = \sum_{j=0}^{+\infty}\mathcal{S}_{A^{j+1}}(e)X^j := S_\infty(X).$$

Proposition 25. *For any error vector $e \in \mathbb{F}_q^{m\ell}$ such that $w(e) \leq \lfloor(\delta-1)/2\rfloor$ we have*

$$\boxed{\Lambda(X)\diamond S_\infty(X) = L(X)}$$

and therefore

$$\Lambda(X)\diamond S_\infty(X) \equiv L(X) \mod X^\delta. \tag{2}$$

We will refer to (2) *as the* key equation.

4.1.1 Problems solving the key equation

In the case of BCH codes, the extended Euclidean and Berlekamp-Massey algorithms can be used to solve the key equation. We denote by $S_\delta(X)$ the polynomial $S_\infty(X) \mod X^\delta$ from (2) which can be written as

$$\begin{pmatrix}\Lambda_0 & \dots & \Lambda_{\delta-1} & \big| & L_0 & \dots & L_{\delta-1}\end{pmatrix}\left(\begin{array}{cccc} S_0 & S_1 & \dots & S_{\delta-1}\\ & S_0 & & \vdots\\ & & \ddots & \vdots\\ & & & S_0\\ \hline -1 & 0 & \dots & 0\\ 0 & -1 & & \vdots\\ \vdots & & \ddots & 0\\ 0 & \dots & 0 & -1\end{array}\right) = 0. \tag{3}$$

Where the S_i's and L_i's are column vectors such that the S_i's are the coefficients of S_δ in $\mathbb{F}_{q^s}^\ell$ and the L_i's are the coefficients in $\mathbb{F}_{q^s}^\ell$ of $L(X)$. The Λ_i's are the coefficients of $\Lambda(X)$ in $M_\ell(\mathbb{F}_{q^s})$. This system of linear equations over $\mathbb{F}_{q^s}$

has many solutions in $\mathbb{F}_{q^s}$ since there are $\ell\delta + \delta$ unknowns and only δ equations for each row of

$$\begin{pmatrix} \Lambda_0 & \dots & \Lambda_{\delta-1} & \mid & L_0 & \dots & L_{\delta-1} \end{pmatrix}.$$

However, we are only interested in the solution such that $(\Lambda_0, \dots, \Lambda_{\delta-1})$ is an error locator polynomial. In other words, if we let $\mathfrak{B}$ be the solutions of (3) and

$$\mathfrak{S} = \left\{ \prod_{i \in W} (1 - A^i X) \in M_\ell(\mathbb{F}_{q^s}) : W \subset \{1, \dots, m\} \text{ and } \#W \leq \lfloor (\delta-1)/2 \rfloor \right\}$$

be the set of all possible locator polynomials corresponding to errors of weight at most $\lfloor (\delta-1)/2 \rfloor$, we are interested in the elements of $\mathfrak{B} \cap \mathfrak{S}$.

Proposition 26. *There exists one and only one solution of equation* (3) *in* $\mathfrak{S}$.

Proof. Equation 2 ensures that there exists at least one element in $\mathfrak{B} \cap \mathfrak{S}$. If there were more than one solution in $\mathfrak{S}$ there would exist more than one codeword in a Hamming ball of radius $\lfloor (\delta-1)/2 \rfloor$ which is absurd. □

The solving of (3) remains difficult. One needs an exponential (in $\ell\delta$) number of arithmetic operations in $\mathbb{F}_{q^s}$ to find the element of $\mathfrak{B} \cap \mathfrak{S}$. For small values of q, ℓ and δ the solution can be found by exhaustive search on the solutions of (3).

4.1.2 Unambiguous decoding scheme

In this subsection, we prove that, as in the BCH case, the roots of the locator polynomial (in $\mathbb{F}_{q^s}[A]$) give precious information about the location of errors. The factorization of polynomials of $M_\ell(\mathbb{F}_{q^s})[X]$ is not unique, all the roots of the locator polynomial do not indicate an error position.

Proposition 27. *Let $e \in \mathbb{F}_q^{m\ell}$ be an error vector such that $w(e) \leq \lfloor (\delta-1)/2 \rfloor$ and $\Lambda(X)$ be the locator polynomial associated to e. We have*

$$e_i \neq 0 \Longleftrightarrow \Lambda(A^{-i}) = 0.$$

Proof. By definition, we have $\Lambda(A^{-i}) = 0$ if $e_i \neq 0$. Conversely, if $e_i = 0$ then $A^j A^{-i} \neq I_\ell$ for $j \in \mathrm{Supp}(e)$. Thus $1 - A^j A^{-i}$ is a unit in $\mathbb{F}_{q^s}[A]$ by definition of A. Therefore $\Lambda(A^{-i}) \neq 0$. □

These roots can be found by an exhaustive search on the powers of A in at most m attempts. At this step the support of the error vector e is known. The last step to complete the decoding is to find the value of the error.

Proposition 28. *Let $e \in \mathbb{F}_q^{m\ell}$ be an error such that $w(e) \leq \lfloor (\delta-1)/2 \rfloor$, $W = \mathrm{Supp}(e)$, $\Lambda(X)$ be the locator and $L(X)$ be the evaluator polynomials associated to e. If A^{-i} is a root of $\Lambda(X)$ for $i \in W$, then*

$$e_i = \prod_{j \in W \setminus \{i\}} (A^i - A^j)^{-1} L(A^{-i})$$

where $L(A^j)$ denotes $\sum (A^j)^i L_i$.

Proof. Let $i_0 \in W$. We have

$$\begin{aligned} L(A^{-i_0}) &= \sum_{i=1}^{w} \prod_{j \neq i}^{w} A_i (1 - A^{-i_0} A_j) y_i \\ &= \prod_{j \in W \setminus \{i_0\}} A^{i_0} (1 - A^{-i_0} A^j) e_{i_0} \\ &= \prod_{j \in W \setminus \{i_0\}} (A^{i_0} - A^j) e_{i_0}. \end{aligned}$$

By definition of A, $A^{i_0} - A^j$ is invertible for all $j \in W$ hence the result. ☐

Algorithm 4.1 Decoding algorithm for quasi-BCH codes

Input: The received word $y = c + e$ where $c \in \mathcal{C}$ and $w(e) \leq \lfloor (\delta - 1)/2 \rfloor$.
Output: The codeword c, if it exists such that $d(y, c) \leq \lfloor (\delta - 1)/2 \rfloor$.

```
  S_δ(X) ← Syndrome of y.
  Compute Λ(X) and L(X) (Subsection 4.1.1).
  ℜ ← roots of Λ(X) in F_{q^s}[A].
  W ← {i | A^{-i} ∈ ℜ}.
  ζ ← (0, ..., 0).
  for i ∈ W do
     ζ_i = ∏_{j∈W\{i}} (A^i − A^j)^{-1} L(A^{-i}).
  end for
  return y − ζ.
```

5 Evaluation codes

5.1 Definition and parameters

In this subsection we generalize evaluation codes. For any ring R and any positive integer k, we denote by $R[X]_{<k}$ the left R-module of all polynomials of $R[X]$ of degree at most $k-1$.

Proposition 29. *Let q be a prime power and ℓ, m be positive integers such that $m = q^\ell - 1$. Let $A \in M_\ell(\mathbb{F}_q)$ be a primitive m-th root of unity. Then $\mathbb{F}_q[A]$ and $\mathbb{F}_{q^\ell}$ are isomorphic as rings.*

Proof. Let $\mu(X)$ be the minimal polynomial of A of degree at most ℓ. We have $\mu | X^m - 1$, thus the roots of μ are all distinct. By Definition 15- (3), the roots of μ lie in $\mathbb{F}_{q^\ell}$ and not in any subfield. Therefore μ is irreducible. ☐

Definition 30 (Quasi-cyclic evaluation codes)**.** Let ℓ be a positive integer and q be a prime power. Let $m = q^\ell - 1$ and $k \leq m$. Let $A \in M_\ell(\mathbb{F}_q)$ a primitive

m-th root of unity. Let π be a $\mathbb{F}_q$-linear map from $\mathbb{F}_q[A]$ into $\mathbb{F}_q^\ell$. We denote by $C_{A,k,\pi}$ the image of:

$$\begin{array}{ccccc} (\mathbb{F}_q[A])[X]_{<k} & \xrightarrow{\mathrm{ev}_A} & (\mathbb{F}_q[A])^m & \xrightarrow{\pi^{\times m}} & (\mathbb{F}_q^\ell)^m \\ P(X) & \longmapsto & \big(P(A^0), \ldots, P(A^{m-1})\big) & \longmapsto & \big(\pi(P(A^0)), \ldots, \pi(P(A^{m-1}))\big). \end{array}$$

Proposition 31. *Taking the notation of Definition 30, $C_{A,k,\pi}$ is a ℓ-quasi cyclic code over $\mathbb{F}_q$ of length $m\ell$ and of dimension over $\mathbb{F}_q$ at least $k\ell - \dim_{\mathbb{F}_q}(\ker \pi^{\times m})$.*

Proof. By Proposition 29 the statement about the dimension of $C_{A,k,\pi}$ is obvious. Let

$$P(X) = \sum_{i=0}^{k-1} \sum_{j=0}^{m-1} P_{ij} A^j X^i \in \mathbb{F}_q[A][X]_{<k}$$

with $P_{ij} \in \mathbb{F}_q$. Then

$$Q(X) = \sum_{i=0}^{k-1} \sum_{j=0}^{m-1} P_{ij} A^{j+i} X^i \in \mathbb{F}_q[A][X]_{<k}$$

is such that $Q(A^i) = P(A^{i+1})$ for all $i \in \mathbb{Z}$ and $C_{A,k,\pi}$ is ℓ-quasi cyclic. $\square$

5.2 New good codes

Proposition 32. *Using the notation of Definition 30, if π is such that for $B = (b_{ij}) \in \mathbb{F}_q[A]$*

- *$\pi(B) = (b_{i1}, \ldots, b_{i\ell})$ for some i,*
- *or $\pi(B) = (b_{1j}, \ldots, b_{\ell j})$ for some j,*

then $\dim C_{A,k,\pi} \geq k\ell$ and $C_{A,k,\pi}$ has minimum distance $d \geq m - k + 1$.

Proof. In both cases, it suffices to notice that $\pi^{\times m}$ is injective. If $\pi^{\times m}(B_1, \ldots, B_m) = 0$ then $\det B_i = 0$ for $i = 1, \ldots, m$. As $\mathbb{F}_q[A]$ is a field we must have $B_i = 0$ for $i = 1, \ldots, m$. In fact under the assumptions of the proposition $\pi^{\times m}$ is an isomorphism since $\#((F_q[A])^m) = q^{m\ell} = \#((F_q^\ell)^m)$. $\square$

Remark 33. All the computations of the examples below have been performed with the MAGMA computer algebra system [3].

1. For some particular choices of π, especially when we decrease the dimension k, we observe that the minimum distance is multiplied by $\ell - 1$. For example, with

$$A = \begin{pmatrix} 0 & \omega & 0 \\ \omega & \omega^2 & \omega^2 \\ 1 & \omega^2 & 1 \end{pmatrix} \in M_3(\mathbb{F}_4) \text{ with } \mathbb{F}_4 = \mathbb{F}_2[\omega],$$

$k = 4$ and $\pi((b_{ij})) = (b_{2,1}, b_{1,2}, b_{2,3})$, we find a $[189, 11, 125]_{\mathbb{F}_4}$-code. According to [9], the previous best known minimum distance was 121.

New codes over $\mathbb{F}_4$				
$[171,11,109]_4$	$[172,11,110]_4$	$[173,11,110]_4$	$[174,11,111]_4$	$[175,11,112]_4$
$[176,11,113]_4$	$[177,11,114]_4$	$[178,11,115]_4$	$[179,11,115]_4$	$[180,11,116]_4$
$[181,11,117]_4$	$[182,11,118]_4$	$[183,11,119]_4$	$[184,10,121]_4$	$[184,11,120]_4$
$[185,10,122]_4$	$[185,11,121]_4$	$[186,10,123]_4$	$[186,11,122]_4$	$[187,10,124]_4$
$[187,11,123]_4$	$[188,10,125]_4$	$[188,11,124]_4$	$[189,10,126]_4$	$[189,11,125]_4$
$[190,10,127]_4$	$[190,11,126]_4$	$[191,10,128]_4$	$[191,11,127]_4$	$[192,11,128]_4$
$[193,11,128]_4$	$[194,11,128]_4$	$[195,11,128]_4$	$[196,11,129]_4$	$[197,11,130]_4$
$[198,11,130]_4$	$[199,11,131]_4$	$[200,11,132]_4$	$[201,10,133]_4$	$[201,11,132]_4$
$[202,10,134]_4$	$[202,11,132]_4$	$[203,10,135]_4$	$[204,10,136]_4$	$[204,11,133]_4$
$[205,11,134]_4$	$[210,11,137]_4$	$[213,11,139]_4$	$[214,11,140]_4$	

Table 1: 49 new codes over $\mathbb{F}_4$ which have a larger minimum distance than the previously known ones.

2. As for Reed-Solomon codes, we can evaluate polynomials of $(\mathbb{F}_q[A])[X]_{<k}$ at less than $m = q^\ell - 1$ points. Following this approach, we find the following new good codes listed below together with the corresponding previous best known minimum distances:

$$\begin{array}{c} [186,11,122]_{\mathbb{F}_4},\ 120; \\ [183,11,119]_{\mathbb{F}_4},\ 117; \\ [180,11,116]_{\mathbb{F}_4},\ 114; \\ [177,11,113]_{\mathbb{F}_4},\ 112. \end{array}$$

3. Markus Grassl applied different methods to construct new codes from our $[189,11,125]_{\mathbb{F}_4}$ code (item 1 of Remark 33). For example, he used a puncturing method [8]. Some of the codes he obtained have the same parameters as the codes listed in item 2 of Remark 33. He found $[186,11,122]_{\mathbb{F}_4}$, $[183,11,119]_{\mathbb{F}_4}$ and $[180,11,116]_{\mathbb{F}_4}$ codes. He also found a $[177,11,114]_{\mathbb{F}_4}$ code while the best known minimum distance was 112. The 49 new codes found with the help of Markus Grassl are listed in Table 1. All the methods used for the construction of these codes are detailed in [9].

Remark 34. We have proved in Proposition 29 that $\mathbb{F}_q[A]$ is a field such that $[\mathbb{F}_q[A] : \mathbb{F}_q] = \ell$. Thus there is a $\mathbb{F}_q$-linear isomorphism from $\mathbb{F}_q[A]$ to $\mathbb{F}_q^\ell$. Consider the following one:

$$\begin{array}{rcl} \mathbb{F}_q[A] & \stackrel{\psi}{\longrightarrow} & \mathbb{F}_q^\ell \\ B = b_0 I_\ell + b_1 A + \cdots + b_{\ell-1} A^{\ell-1} & \longmapsto & (b_0, b_1, \ldots, b_{\ell-1}). \end{array}$$

Then

$$C_{A,k,\psi} = \psi^{\times m}(\mathrm{ev}_A(\mathbb{F}_q[A][X]_{<k}))$$

is still an ℓ-quasi cyclic code of length $m\ell$ and of dimension $k\ell$. Let $\Pi \in M_\ell(\mathbb{F}_q)$ and let

$$\begin{array}{rcl} \pi : \mathbb{F}_q^\ell & \to & \mathbb{F}_q^\ell \\ x & \mapsto & x\Pi \end{array}$$

for a given $\Pi \in M_\ell(\mathbb{F}_q)$. Then

$$C_{A,k,\psi,\pi} = \pi^{\times m}(\psi^{\times m}(\mathrm{ev}_A(\mathbb{F}_q[A][X]_{<k})))$$

is an ℓ-quasi cyclic code of length $m\ell$ and dimension $\geq k\ell - \dim(\ker \pi)$.

We notice that there exist matrices Π for which the obtained minimum distance is always greater than $m - k + 1$. For instance, taking $\ell = 3$, $q = 4$ and the matrix

$$\Pi = \begin{pmatrix} 1 & \omega^2 & \omega \\ \omega^2 & \omega & 1 \\ 1 & 1 & 1 \end{pmatrix},$$

give codes with minimum distance close to $2(m - k + 1)$.

6 Conclusion

In this paper we presented a generalization of results for cyclic codes to quasi-cyclic codes. We proved that there is a natural one-to-one correspondence between ℓ-quasi-cyclic codes and left ideals of $M_\ell(\mathbb{F}_q)[X]/(X^m - 1)$. We then extended the construction of BCH and evaluation codes to this context. This generalization allowed us to find a lot of new codes with good parameters and, sometimes, beating previous known minimum distances. A deeper study of decoding algorithms for quasi-BCH need more work and remains an open problem.

Acknowledgments

We would like to thank the referees, whose suggestions have permit to improve this article, in particular, for Algorithm 2.2 and for the idea of using the Morita equivalence to prove the one-to-one correspondence between left ideals and quasi-cyclic codes. We would like to thank Markus Grassl for his precious help for finding new good codes.

References

[1] D. Augot, M. Barbier, and A. Couvreur. List-decoding of binary Goppa codes up to the binary Johnson bound. In *Information Theory Workshop (ITW), 2011 IEEE*, pages 229–233, oct 2011.

[2] T. Berger, P.-L. Cayrel, P. Gaborit, and A. Otmani. Reducing Key Length of the McEliece Cryptosystem. In *Proceedings of the 2nd International Conference on Cryptology in Africa: Progress in Cryptology*, AFRICACRYPT '09, pages 77–97, Berlin, Heidelberg, 2009. Springer-Verlag.

[3] Wieb Bosma, John Cannon, and Catherine Playoust. The Magma algebra system. I. The user language. *J. Symbolic Comput.*, 24(3-4):235–265, 1997. Computational algebra and number theory (London, 1993).

[4] N. Bourbaki. *Algèbre: Chapitre 8*. Springer Verlag, 2011.

[5] P.-L. Cayrel, C. Chabot, and A. Necer. Quasi-cyclic codes as codes over rings of matrices. *Finite Fields and Their Applications*, 16(2):100–115, 2010.

[6] C. Chabot. Factorisation in $M_\ell(\mathbb{F}_q)[X]$. Construction of quasi-cyclic codes. In *WCC 2011 - Workshop on coding and cryptography*, pages 209–218, Paris, France, apr 2011.

[7] J.-C. Faugère, A. Otmani, L. Perret, and J.-P. Tillich. Algebraic Cryptanalysis of McEliece Variants with Compact Keys. In Henri Gilbert, editor, *Advances in Cryptology EUROCRYPT 2010*, volume 6110 of *Lecture Notes in Computer Science*, pages 279–298. Springer Berlin / Heidelberg, 2010.

[8] M. Grassl and G. White. New good linear codes by special puncturings. In *Information Theory, 2004. ISIT 2004. Proceedings. International Symposium on*, page 454, jun 2004.

[9] Markus Grassl. Bounds on the minimum distance of linear codes and quantum codes. Online available at http://www.codetables.de, 2007. Accessed on 2011-04-19.

[10] K. Lally and P. Fitzpatrick. Algebraic structure of quasicyclic codes. *Discrete Applied Mathematics*, 111(1–2):157–175, 2001.

[11] S. Lang. *Algebra*, volume 211 of *Graduate Texts in Mathematics*. Springer-Verlag, third edition, 2002.

[12] Y. X. Li, R. H. Deng, and X. M. Wang. On the equivalence of McEliece's and Niederreiter's public-key cryptosystems. *IEEE Trans. Inform. Theory*, 40(1):271–273, January 1994.

[13] S. Ling and P. Solé. On the algebraic structure of quasi-cyclic codes .I. Finite fields. *IEEE Trans. Inform. Theory*, 47(7):2751–2760, nov 2001.

[14] S. Ling and P. Solé. Good self-dual quasi-cyclic codes exist. *IEEE Trans. Inform. Theory*, 49(4):1052–1053, april 2003.

[15] F.J. MacWilliams and N.J.A. Sloane. *The theory of error-correcting codes*. North-Holland mathematical library. North-Holland, 1986.

[16] R. McEliece. A Public-Key Cryptosystem Based On Algebraic Coding Theory. *Deep Space Network Progress Report*, 44:114–116, 1978.

[17] H. Niederreiter. Knapsack-type cryptosystems and algebraic coding theory. *Problems of Control and Information Theory*, 15(2):159–166, 1986.

[18] V. G. Umaña and G. Leander. Practical Key Recovery Attacks On Two McEliece Variants. In Carlos Cid and Jean-Charles Faugére, editors, *Proceedings of the Second International Conference on Symbolic Computation and Cryptography*, pages 27–44, June 2010.